

ARS MATHEMATICA  
CONTEMPORANEAAlso available at <http://amc.imfm.si>

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)

ARS MATHEMATICA CONTEMPORANEA 3 (2010) 201–214

# Asymptotic automorphism groups of Cayley digraphs and graphs of abelian groups of prime-power order

Edward Dobson

*Department of Mathematics and Statistics, Mississippi State University  
PO Drawer MA Mississippi State, MS 39762*

Received 6 October 2009, accepted 21 October 2010, published online 17 November 2010

---

## Abstract

We show that almost every Cayley graph  $\Gamma$  of an abelian group  $G$  of odd prime-power order has automorphism group as small as possible. Additionally, we show that almost every Cayley (di)graph  $\Gamma$  of an abelian group  $G$  of odd prime-power order that does not have automorphism group as small as possible is a normal Cayley (di)graph of  $G$  (that is,  $G_L \triangleleft \text{Aut}(\Gamma)$ ).

*Keywords:* Cayley graph, abelian group, automorphism group, asymptotic,  $p$ -group

*Math. Subj. Class.:* 05C25

---

Determining the full automorphism group of a Cayley graph or digraph is one of the most fundamental questions that one can ask about a Cayley graph. While it is usually quite difficult to determine the automorphism group of a Cayley graph or digraph, somewhat surprisingly for some rather general groups  $G$  it has been shown that *almost* every Cayley graph and digraph of the groups in these classes has automorphism group as small as possible. That is, if  $\Gamma$  is a Cayley (di)graph of  $G$ , then with probability approaching 1 as  $|G| \rightarrow \infty$ , the automorphism group of  $\Gamma$  is  $G_L$ . Indeed, while working on the problem (now solved, see [15] for graphs and [3, 4] for digraphs) of determining which groups  $G$  have a digraphical regular representation (a Cayley digraph  $\Gamma$  of  $G$  with automorphism group  $\text{Aut}(\Gamma) = G$ ), or DRR, and which groups  $G$  have a graphical regular representation (a Cayley graph  $\Gamma$  of  $G$  with  $\text{Aut}(\Gamma) = G$ ), or GRR, Babai, Godsil, Imrich, and Lovász (see [5]) conjectured that unless  $G$  is an abelian or a generalized dicyclic group, almost all Cayley digraphs of  $G$  are GRR's, while for digraphs, the conjecture is that almost all Cayley graphs of  $G$  are DRR's. (For graphs, it is known that no Cayley graphs of groups that are not elementary abelian 2-groups nor dicyclic are GRR's.)

---

*E-mail address:* [dobson@math.msstate.edu](mailto:dobson@math.msstate.edu) (Edward Dobson)

In terms of verifying these conjectures, in 1981 Godsil [16] showed that almost all Cayley digraphs of groups  $G$  of prime-power order are DRR's provided that there is no homomorphism from  $G$  onto  $\mathbb{Z}_p \wr \mathbb{Z}_p$ . Additionally, Babai and Godsil [5] proved that almost every Cayley digraph of a nilpotent group  $G$  is a DRR. Godsil [16] showed that for every other group  $G$  (i.e.  $G$  is not abelian nor generalized dicyclic) of prime-power order with no homomorphism onto  $\mathbb{Z}_p \wr \mathbb{Z}_p$ , almost all Cayley graphs of  $G$  are GRR's, while Babai and Godsil [5] showed that for every nilpotent but not abelian group  $G$ , almost every Cayley graph of  $G$  is a GRR. Babai and Godsil also considered whether or not almost all Cayley graphs of an abelian group  $G$  has automorphism group as small as possible (namely of order  $2|G|$ ), and showed that this was indeed the case for almost all such Cayley graphs provided that the order of  $G$  is congruent to 3 modulo 4.

In this paper, we will consider the asymptotic automorphism groups of Cayley graphs and digraphs of abelian groups of odd prime-power order. First, as it will not involve much additional work, we will prove in Theorem 1.7 the known result that almost all Cayley digraphs of an abelian group  $G$  of odd prime-power order have automorphism group  $G_L$ . In Theorem 3.3 we show that almost all Cayley graphs of an abelian group  $G$  of odd prime-power order have automorphism groups as small as possible, namely of order  $2|G|$ , removing the restriction that  $|G| \equiv 3 \pmod{4}$  for these groups. M.-Y. Xu [27] introduced the notion of a *normal Cayley (di)graph of a group  $G$* , that is, a Cayley (di)graph  $\Gamma$  of a group  $G$  such that  $G_L \triangleleft \text{Aut}(\Gamma)$ , and he conjectured that almost all Cayley (di)graphs of a group  $G$  are normal Cayley digraphs of  $G$ . Of course, if almost all Cayley (di)graphs of  $G$  are GRR's or DRR's, then almost all Cayley (di)graphs of a group  $G$  are normal Cayley digraphs of  $G$ , so Xu's conjecture is weaker than the conjectures in the previous paragraph. We conjecture (Conjecture 4.1) that almost every Cayley (di)graph of  $G$  whose automorphism group is not as small as possible is a normal Cayley (di)graph of  $G$ , and verify this conjecture for graphs (Theorem 3.5) and digraphs (Theorem 2.9) of abelian groups of odd prime-power order. We finish with a few additional problems that can be considered to try to understand more fully the asymptotic behavior automorphism groups of Cayley (di)graphs.

One final comment is in order about what we mean by “almost all” Cayley digraphs. In this paper, we first fix a specific abelian group of odd prime-power order. In order then for the number of group elements to go to infinity without changing the structure of the group, we must let  $p$  approach infinity.

## 1 DRR's

In this section, we develop some elementary tools that will be needed for the main results. Additionally, as it will not take much extra work, we prove that almost every Cayley digraph of an abelian group of prime-power order is a DRR - a special case of a result of Godsil as mentioned above - for completeness.

**Definition 1.1.** Let  $G$  be a group and  $S \subset G$ . We define the Cayley digraph of  $G$  with connection set  $S$  to be the digraph  $\Gamma = \Gamma(G, S)$  defined by  $V(\Gamma) = G$  and  $E(\Gamma) = \{(g, gs) : s \in S, g \in G\}$ . If  $S = S^{-1}$ , then  $\Gamma$  is a Cayley graph of  $G$  with connection set  $S$ . Note that  $G_L = \{x \rightarrow gx : g \in G\} \leq \text{Aut}(\Gamma)$ .

**Lemma 1.2.** Let  $G$  be a group of finite order  $n$  and  $\alpha \in \text{Aut}(G)$ ,  $\alpha \neq 1$ . Then  $\alpha$  has at most  $3n/4$  orbits in its natural action on  $G$ .

*Proof.* It is easy to see that the set of all fixed points of  $\alpha$  forms a subgroup  $H$  of  $G$ . Then  $|H| \leq n/2$ . As each orbit contained in  $G - H$  has order at least 2, we see that the number of orbits of  $\alpha$  is at most

$$|H| + |G - H|/2 = |H|/2 + |G|/2 \leq 3n/4.$$

□

Similarly, we also have the following result.

**Lemma 1.3.** *Let  $G$  be a group of order  $p^k$ ,  $p$  a prime, and  $\alpha \in \text{Aut}(G)$  such that  $|\alpha|$  has order a power of  $p$ . Then  $\alpha$  has at most  $2p^{k-1} - p^{k-2}$  orbits.*

*Proof.* As in the previous result, the set of all fixed points of  $\alpha$  forms a subgroup  $H$  of  $G$ , and so  $|H| \leq p^{k-1}$ . Also, as  $\alpha$  has order a power of  $p$ , each orbit contained in  $G - H$  has order at least  $p$ . We see that the number of orbits of  $\alpha$  is at most

$$|H| + \frac{|G - H|}{p} \leq p^{k-1} + \frac{p^k - p^{k-1}}{p} = 2p^{k-1} - p^{k-2}.$$

□

We shall have need of the following result.

**Lemma 1.4.** *Let  $G$  be a group of prime-power order  $p^k$ . Then  $|\text{Aut}(G)| \leq |\text{Aut}(\mathbb{Z}_p^k)|$ .*

*Proof.* Let  $M$  be a minimal set of generators of  $G$ , with  $j = |M|$ . By [18, Chapter III, Satz 3.19],

$$|\text{Aut}(G)| \leq p^{j(k-j)} \prod_{i=0}^{j-1} (p^j - p^i) = \prod_{i=0}^{j-1} (p^k - p^i p^{k-j}) \leq \prod_{i=0}^{j-1} (p^k - p^i) = |\text{Aut}(\mathbb{Z}_p^k)|.$$

□

**Lemma 1.5.** *Let  $k$  be fixed a positive integer. Then there exists an integer  $N$  such that if  $p^k \geq N$ , then  $|\text{Aut}(\mathbb{Z}_p^k)| \leq 2p^k/8$ .*

*Proof.* Clearly there exists a positive integer  $N$  such that if  $x \geq N$ , then  $x^k \leq 2x/8$ . Letting  $p$  be the smallest prime number such that  $p^k \geq x \geq N$ , we see that  $p^{k^2} \leq 2p^k/8$ . Then

$$|\text{Aut}(\mathbb{Z}_p^k)| = \prod_{i=0}^{k-1} (p^k - p^i) \leq p^{k^2} \leq 2p^k/8.$$

□

**Definition 1.6.** For a group  $G$ , we define  $\text{CayDi}(G)$  to be the set of all Cayley digraphs of  $G$ , and  $\text{DRR}(G)$  to be the set of all Cayley digraphs of  $G$  which are digraphical regular representations of  $G$ . Similarly, we let  $\text{Cay}(G)$  be the set of all Cayley graphs of  $G$ , and  $\text{GRR}(G)$  to be the set of all Cayley graphs of  $G$  which are graphical regular representations of  $G$ .

**Theorem 1.7.** *Almost every digraph of an abelian group  $G$  of prime-power order  $p^k$  is a DRR. More specifically,*

$$\lim_{p \rightarrow \infty} \frac{|DRR(G)|}{|CayDi(G)|} = 1.$$

*Proof.* Let  $G$  be an abelian group of order  $p^k$  and  $\Gamma$  a Cayley digraph of  $G$ . If  $N_{\text{Aut}(\Gamma)}(G_L) = G_L$ , then a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$  must have order  $p^k$ , and so  $G_L$  is contained in the center of its normalizer. By Burnside’s Transfer Theorem [17, Theorem 7.4.3],  $\text{Aut}(\Gamma)$  has a normal  $p$ -complement  $H$ . As  $H \triangleleft \text{Aut}(\Gamma)$ , the orbits of  $H$  form a complete block system  $\mathcal{B}$  of  $\text{Aut}(\Gamma)$ , and as the size of an orbit of  $H$  divides  $|H|$ , we have that blocks of  $\mathcal{B}$  consist of blocks of size relatively prime to  $p$ . As  $\Gamma$  has order  $p^k$ , we see that  $\mathcal{B}$  consists of  $p^k$  blocks of size 1. Thus  $H = 1$  and  $\text{Aut}(\Gamma) = G_L$ . That is, if  $N_{\text{Aut}(\Gamma)}(G_L) = G_L$ , then  $\Gamma$  is a DRR of  $G$ .

We now provide an upper bound on the number of Cayley digraphs of  $G$  that are not DRR’s of  $G$ , provided that  $p^k \geq N$ , where  $N$  is as given by Lemma 1.5. Let  $\Gamma$  be such a digraph. By the argument in the preceding paragraph,  $N_{\text{Aut}(\Gamma)}(G_L) \neq G_L$ . As  $N_{S_G}(G_L) = \text{Aut}(G) \cdot G_L$  [8, Corollary 4.2B], we see that  $\text{Aut}(\Gamma)$  contains a nontrivial group automorphism  $\alpha$  of  $G$ . By Lemma 1.2,  $\alpha$  has at most  $3p^k/4$  orbits, and as the connection set of  $\Gamma$  must consist of unions of orbits of  $\alpha$ , we see that there are at most  $2^{3p^k/4}$  Cayley digraphs of  $G$  whose automorphism group contains  $\alpha$ . By Lemma 1.4, there are at most  $|\text{Aut}(\mathbb{Z}_p^k)|$  possible choices of  $\alpha$ , and by Lemma 1.5,  $|\text{Aut}(\mathbb{Z}_p^k)| \leq 2^{p^k/8}$ . We conclude that there are at most  $2^{3p^k/4} \cdot 2^{p^k/8} = 2^{7p^k/8}$  Cayley digraphs of  $G$  that are not DRR’s of  $G$ . As there are  $2^{p^k}$  distinct Cayley digraphs of  $G$ , we see that

$$\lim_{p \rightarrow \infty} \frac{|DRR(G)|}{|CayDi(G)|} \geq \lim_{p \rightarrow \infty} \frac{2^{p^k} - 2^{7p^k/8}}{2^{p^k}} = 1.$$

□

## 2 Normal Cayley Digraphs

In this section we consider the question of whether or not almost all Cayley digraphs of an abelian group of prime-power order are normal Cayley digraphs.

**Definition 2.1.** Let  $\Gamma$  be a Cayley digraph of  $G$ . We say that  $\Gamma$  is a normal Cayley digraph of  $G$  if  $G_L \triangleleft \text{Aut}(\Gamma)$ . For a group  $G$ , we denote the set of all normal Cayley digraphs of  $G$  by  $NorCayDi(G)$ . The set of all normal Cayley graphs of  $G$  will be denoted by  $NorCay(G)$ .

**Definition 2.2.** Let  $G$  be an abelian group of prime-power order  $p^k$ , so that  $G \cong \prod_{i=1}^r \mathbb{Z}_{p^{a_i}}$ , where  $\sum_{i=1}^r a_i = k$ . We define the number of elementary divisors of  $G$  to be  $r$ , and say  $G$  is of rank  $r$ .

**Definition 2.3.** For  $H \leq G$ , we define the normal closure of  $H$  in  $G$ , denoted by  $H^G$ , to be  $\langle g^{-1}hg : g \in G, h \in H \rangle$ .

Note that  $H^G \triangleleft G$ , and is the smallest normal subgroup of  $G$  that contains  $H$ .

The following result is [10, Theorem 6.3], and from it, we will obtain the main tool (Lemma 2.6) used for the rest of the work in this paper.

**Theorem 2.4.** *Let  $G \leq S_{p^k}$  be transitive with an abelian Sylow  $p$ -subgroup  $P$  of rank  $t$ . If  $p > 2^{t-1}$ , then  $P^G$  is permutation isomorphic to a direct product of cyclic groups and doubly-transitive nonabelian simple groups with the canonical action, with the number of factors in the direct product equal to  $t$ .*

**Definition 2.5.** Let  $\Omega$  be a set and  $G \leq S_\Omega$ . Let  $G$  act on  $\Omega \times \Omega$  by  $g(\omega_1, \omega_2) = (g(\omega_1), g(\omega_2))$  for every  $g \in G$  and  $\omega_1, \omega_2 \in \Omega$ . We define the 2-closure of  $G$ , denoted  $G^{(2)}$ , to be the largest subgroup of  $S_\Omega$  whose orbits on  $\Omega \times \Omega$  are the same as  $G$ 's. Let  $\mathcal{O}_1, \dots, \mathcal{O}_r$  be the orbits of  $G$  acting on  $\Omega \times \Omega$ . Define digraphs  $\Gamma_1, \dots, \Gamma_r$  by  $V(\Gamma_i) = \Omega$  and  $E(\Gamma_i) = \mathcal{O}_i$ . Each  $\Gamma_i$ ,  $1 \leq i \leq r$ , is an orbital digraph of  $G$ , and it is straightforward to show that  $G^{(2)} = \cap_{i=1}^r \text{Aut}(\Gamma_i)$ . Clearly the automorphism group of a graph or digraph is 2-closed.

**Lemma 2.6.** *Let  $k$  be a positive integer, and  $p$  a prime such that  $p > 2^{k-1}$ . Let  $G \leq S_{p^k}$  be transitive and 2-closed with Sylow  $p$ -subgroup  $P$  that is abelian. Then one of the following is true:*

1.  $G$  has a normal Sylow  $p$ -subgroup, or
2.  $G$  contains a normal subgroup that is permutation isomorphic to  $S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has an abelian Sylow  $p$ -subgroup.

*Proof.* As  $p > 2^{k-1} \geq 2^{t-1}$ , where  $t$  is the rank of  $P$ , we may apply Theorem 2.4. Then either the result follows or  $P^G$  is permutation isomorphic to a direct product of cyclic groups and doubly-transitive nonabelian simple groups with the canonical action, with the number of factors in the direct product equal to  $t$ . As if  $H$  is doubly-transitive of degree  $n$ , then  $H^{(2)} = S_n$  and a regular group is 2-closed, by [19] (this result also appears in [7, Theorem 5.1]), we have that  $(P^G)^{(2)} \leq G^{(2)} = G$  is a direct product of cyclic groups and symmetric groups. If any of these symmetric groups are of composite degree, then clearly a Sylow  $p$ -subgroup of  $(P^G)^{(2)}$  cannot be abelian, as a Sylow  $p$ -subgroup of  $S_{p^i}$ ,  $i \geq 2$ , is nonabelian. Thus  $G$  is a direct product of cyclic groups and symmetric groups of prime degree, and the result follows. □

The following result counts the number of Cayley digraphs of  $G$  whose automorphism group does not contain a regular Sylow  $p$ -subgroup. That is, it counts the number of Cayley digraphs of an abelian group for which the previous result does not apply.

**Lemma 2.7.** *Let  $G$  be an abelian group of prime-power order  $p^k$ . Then there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{2p^{k-1} - p^{k-2}}$  Cayley digraphs  $\Gamma$  of  $G$  such that a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$  is not  $G_L$ .*

*Proof.* If  $G_L$  is not a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$ , then  $N_{\text{Aut}(\Gamma)}(G_L)$  contains an element of order  $p$  that is not in  $G_L$  by a Sylow Theorem. As  $N_{S_G}(G_L) = \text{Aut}(G) \cdot G_L$  [8, Corollary 4.2B], we conclude that  $\text{Aut}(\Gamma)$  contains an element  $\alpha$  of order  $p$  that is also an element of  $\text{Aut}(G)$ . By Lemma 1.3, we have that  $\alpha$  has at most  $2p^{k-1} - p^{k-2}$  orbits. As  $\alpha \in \text{Aut}(\Gamma)$  if and only if the connection set of  $\Gamma$  is a union of orbits of  $\alpha$ , we conclude that there are at most  $2^{2p^{k-1} - p^{k-2}}$  Cayley digraphs of  $G$  whose automorphism group contains  $\alpha$ . By Lemma 1.4,  $|\text{Aut}(G)| \leq |\text{Aut}(\mathbb{Z}_p^k)|$ , and so there are at most  $|\text{Aut}(\mathbb{Z}_p^k)|$  choices for  $\alpha$ . The result then follows. □

**Lemma 2.8.** *Let  $P$  be an abelian group of order  $p^k$ . The number of Cayley digraphs of  $P$  whose automorphism group has Sylow  $p$ -subgroup  $P$  and contains a subgroup permutation isomorphic to  $S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has an abelian Sylow  $p$ -subgroup, is at most  $|\text{Aut}(P)| \cdot 2^{2p^{k-1}} \leq |\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{2p^{k-1}}$ .*

*Proof.* Assume for the moment that  $P = \mathbb{Z}_p \times P_1$ , where  $P_1$  is an abelian group of order  $p^{k-1}$ . Let  $a \in \mathbb{Z}_p^*$  be of order  $p - 1$  and  $\alpha : \mathbb{Z}_p \times P_1 \rightarrow \mathbb{Z}_p \times P_1$  by  $\alpha(i, j) = (ai, j)$ . Then  $\alpha \in \text{Aut}(P)$  and  $\alpha \in S_p \times A$ . We conclude that if  $\Gamma$  is a Cayley digraph of  $P$  with connection set  $S$  such that  $\text{Aut}(\Gamma) \geq S_p \times A$ , then  $S$  is a union of orbits of  $\alpha$ . As  $\alpha$  has  $2p^{k-1}$  orbits, there are at most  $2^{2p^{k-1}}$  Cayley digraphs of  $P$  whose automorphism group contains  $S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has an abelian Sylow  $p$ -subgroup. Now let  $\Gamma$  be a Cayley digraph of  $P$  whose automorphism group contains a subgroup permutation isomorphic to  $S_p \times A$ ,  $A \leq S_{p^{k-1}}$  with an abelian Sylow  $p$ -subgroup. Then there exists (see [8, Exercise 1.6.1])  $g \in S_{p^k}$  such that  $g^{-1}\text{Aut}(\Gamma)g \geq S_p \times A$ . Then  $\text{Aut}(g^{-1}(\Gamma)) \geq S_p \times A$ . We also note that  $g^{-1}(\Gamma)$  is a Cayley digraph of  $P$  as  $P \leq S_p \times A$  [25]. As  $P$  is a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$ , we have by [2, Lemma 3.1] and a Sylow Theorem that there exists  $\beta \in \text{Aut}(P)$  such that  $\beta(\Gamma) = g^{-1}(\Gamma)$ . We conclude that  $\beta\text{Aut}(\Gamma)\beta^{-1} = \text{Aut}(g^{-1}(\Gamma))$  or that  $\text{Aut}(\Gamma) \geq \beta^{-1}(S_p \times A)\beta$ . Thus if  $\Gamma$  is a Cayley digraph of  $P$  whose automorphism group contains a subgroup permutation isomorphic to  $S_p \times A$ , then  $\Gamma$  is the image under a group automorphism of  $P$  of a Cayley digraph of  $P$  whose automorphism group contains  $S_p \times A$ . As there are at most  $2^{2p^{k-1}}$  Cayley digraphs of  $P$  whose automorphism group contains  $S_p \times A$ , there are at most  $|\text{Aut}(P)| \cdot 2^{2p^{k-1}}$  Cayley digraphs of  $P$  whose automorphism group contains a subgroup permutation isomorphic to  $S_p \times A$ . The result then follows by Lemma 1.4. □

**Theorem 2.9.** *Let  $G$  be an abelian group of prime-power order  $p^k$ . Then almost every Cayley digraph of  $G$  that is not a DRR is a normal Cayley digraph of  $G$ . In particular,*

$$\lim_{p \rightarrow \infty} \frac{|\text{NorCayDi}(G) - \text{DRR}(G)|}{|\text{CayDi}(G) - \text{DRR}(G)|} = 1.$$

*Proof.* Choose  $p$  so that  $p \geq 2^{k-1}$ . Then, according to Lemma 2.6, if  $\Gamma$  is a non-normal Cayley digraph of  $G$ , then either  $G_L$  is not a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$ , or  $\text{Aut}(\Gamma)$  contains a subgroup isomorphic to  $S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has an abelian Sylow  $p$ -subgroup. Let  $\iota \in \text{Aut}(G)$  be given by  $\iota(i, j) = (-i, -j)$ . Note that  $\iota$  has 1 orbit of size 1 and  $(p^k - 1)/2$  orbits of size 2. Thus  $\iota$  has  $(p^k + 1)/2$  orbits. As  $\iota \in \text{Aut}(G)$  and fixes  $(0, 0)$ , if  $\Gamma$  is a Cayley digraph of  $G$  with connection set  $S$ , then  $\iota \in \text{Aut}(\Gamma)$  if and only if  $\iota(S) = S$ . Thus  $\iota \in \text{Aut}(\Gamma)$  if and only if  $S$  is a union of orbits of  $\iota$ . We conclude that there are at least  $2^{(p^k+1)/2}$  distinct Cayley digraphs of  $G$  that are not DRR's of  $G$ .

By Lemma 2.8, there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{2p^{k-1}}$  Cayley digraphs of  $P$  whose automorphism group is permutation isomorphic to  $S_p \times A$ . As by Lemma 2.7 there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{p^{k-1}-p^{k-2}}$  Cayley digraphs  $\Gamma$  of  $G$  such that  $G_L$  is not a Sylow  $p$ -subgroup of  $G$ , we conclude by Lemma 2.6 that there are at most

$$|\text{Aut}(\mathbb{Z}_p^k)|(2^{2p^{k-1}} + 2^{p^{k-1}-p^{k-2}})$$

Cayley digraphs of  $G$  that are not normal Cayley digraphs of  $G$ . Then

$$\begin{aligned} \lim_{p \rightarrow \infty} \frac{|NorCayDi(G)|}{|CayDi(G) - DRR(G)|} &\geq 1 - \lim_{p \rightarrow \infty} \frac{|\text{Aut}(\mathbb{Z}_p^k)|(2^{2p^{k-1}} + 2^{p^{k-1}-p^{k-2}})}{2^{(p^k+1)/2}} \\ &\geq 1 - \lim_{p \rightarrow \infty} \frac{2^{p^k/8}(2^{2p^{k-1}} + 2^{p^{k-1}-p^{k-2}})}{2^{(p^k+1)/2}} \\ &= 1 \end{aligned}$$

by Lemma 1.5. □

We remark that the above argument also shows that almost every Cayley graph of an abelian group of prime-power order is a normal Cayley graph of  $G$ . Indeed, if there are at most

$$|\text{Aut}(\mathbb{Z}_p^k)|(2^{2p^{k-1}} + 2^{p^{k-1}-p^{k-2}})$$

Cayley digraphs of  $G$  that are not normal Cayley digraphs of  $G$ , there are at most the same number of Cayley graphs of  $G$  that are not normal Cayley graphs of  $G$ . Also,  $2^{(p^k+1)/2}$  is the number of Cayley graphs of  $G$ , and so

$$\lim_{p \rightarrow \infty} \frac{|NorCay(G)|}{|Cay(G)|} = 1.$$

### 3 Almost all Cayley graphs have automorphism group as small as possible

We begin with a technical result which will allow us to determine an upper bound on the number of Cayley graphs of abelian groups of prime-power order whose automorphism groups are not as small as possible.

**Lemma 3.1.** *Let  $G$  be an abelian group of odd prime-power order  $p^k$ ,  $p$  a prime, and  $\beta \in \text{Aut}(G)$  be given by  $\beta(i) = -i$ . Let  $\alpha \in \text{Aut}(G)$  such that  $\alpha \neq \beta$ . Then  $\langle \alpha, \beta \rangle$  has at most  $1 + p^{k-1}/2 + p^k/4$  orbits. If  $|\alpha| = r$  is relatively prime to 2, then  $\langle \alpha, \beta \rangle$  has at most  $1 + p^{k-1}/2 + (p^k - p^{k-1})/(2r')$  orbits, where  $r'$  is the smallest divisor of  $r$  greater than one.*

*Proof.* First observe that  $\beta$  has exactly one orbit of one element, and  $(p^k - 1)/2$  orbits of size 2. Additionally,  $\alpha$  commutes with  $\beta$ , as, writing the group operation multiplicatively,  $\alpha\beta(i) = \alpha(i^{-1}) = \alpha^{-1}(i) = \beta\alpha(i)$ . We conclude that every orbit of  $\langle \alpha, \beta \rangle$  has order dividing  $|\langle \alpha, \beta \rangle|$  which divides  $|\alpha| \cdot |\beta|$ . Clearly  $\langle \alpha, \beta \rangle$  has only one orbit of size 1 as  $\beta$  only has one orbit of size 1. Let  $\mathcal{O}$  be a nontrivial orbit of  $\langle \alpha, \beta \rangle$ . Then  $\beta|_{\mathcal{O}}$  has order 2, and so  $|\mathcal{O}| = 2$ , or  $|\langle \alpha, \beta \rangle|_{\mathcal{O}} \geq 4$ . If  $|\mathcal{O}| = 2$ , then  $\alpha|_{\mathcal{O}} \in \langle \beta \rangle|_{\mathcal{O}}$ . Thus every element of  $\mathcal{O}$  is a fixed point of  $\alpha$  or for every  $i \in \mathcal{O}$ ,  $\alpha(i) = \beta(i)$ . Thus every element of  $\mathcal{O}$  is either a fixed point of  $\alpha$  or a fixed point of  $\alpha\beta^{-1}$ . As the set of fixed points of an automorphism of  $G$  forms a subgroup of  $G$ , each of  $\alpha$  and  $\alpha\beta^{-1}$  has at most  $p^{k-1}$  fixed points, and so there are at most  $2p^{k-1}$  elements of  $G$  that are contained in orbits of  $\langle \alpha, \beta \rangle$  of order 2 (actually, there are fewer, as the identity in  $G$  is counted among these  $2p^{k-1}$  points as it is a fixed point of both  $\beta$  and  $\alpha\beta^{-1}$ ). There are thus at most  $p^k - 2p^{k-1}$  elements in  $G$  that are contained in orbits of size at least 4. Then  $G$  has at most  $1 + 2p^{k-1}/2 + (p^k - 2p^{k-1})/4 =$



$1 + p^{k-1}/2 + p^k/4$  orbits. As  $|\alpha| = r \neq 2$ , as above,  $\langle \alpha, \beta \rangle$  has one orbit of size one. Also,  $\alpha$  has at most  $p^{k-1}$  fixed points, and so there are at most  $p^{k-1}/2$  orbits of size 2. By arguments analogous to those above, every other point is contained in orbits of size  $2r'' > 1$ , where  $r''$  is a divisor of  $r$ . Thus if  $r'$  is the smallest divisor of  $r$  greater than one, then there are at most  $(p^k - p^{k-1})/(2r')$  such orbits. As  $|\alpha| = r \neq 2$ ,  $\alpha$  has at most  $1 + p^{k-1}/2 + (p^k - p^{k-1})/(2r')$  orbits.  $\square$

We remark that if  $r = p$  in the previous result, then  $1 + p^{k-1}/2 + (p^k - p^{k-1})/2r = 1 + p^{k-1} - p^{k-2}/2$ .

**Definition 3.2.** Let  $G$  be an abelian group that is not an elementary abelian 2-group. We define  $Small(G)$  to be the set of all Cayley graphs  $\Gamma$  of  $G$  such that  $|\text{Aut}(\Gamma)| = 2 \cdot |G|$ . That is,  $Small(G)$  is the set of all Cayley graphs of  $G$  whose automorphism groups are as small as possible.

**Theorem 3.3.** Let  $G$  be an abelian group of prime-power order. Then almost every Cayley graph of  $G$  has automorphism group of order  $2 \cdot |G|$ . More specifically,

$$\lim_{p \rightarrow \infty} \frac{|Small(G)|}{|Cay(G)|} = 1.$$

*Proof.* Let  $\Gamma$  be a Cayley graph of  $G$ , where  $G$  is an abelian group of prime-power order  $p^k$ ,  $p \geq 3$  a prime. As  $\Gamma$  is a graph, the map  $\beta \in \text{Aut}(G)$  given by  $\beta(i) = -i$  is contained in  $\text{Aut}(\Gamma)$ . As  $|\beta| = 2$  and has exactly one fixed point, there are  $(p^k + 1)/2$  orbits of  $\beta$  and so there are  $2^{(p^k+1)/2}$  Cayley graphs of  $G$ . If a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$  has order at least  $p^{k+1}$ , then by a Sylow Theorem,  $N_{\text{Aut}(\Gamma)}(G_L)$  has order at least  $p^{k+1}$ . As  $N_{S_G}(G_L) = \text{Aut}(G) \cdot G_L$ , we have that  $\text{Aut}(\Gamma)$  contains an automorphism  $\alpha \neq \beta$ . If a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$  has order  $p^k$ , then by Lemma 2.6, we have that either  $\Gamma \in Small(G)$ , there exists  $\beta \neq \alpha \in \text{Aut}(\Gamma) \cap \text{Aut}(G)$ , or  $\text{Aut}(\Gamma) \geq S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has Sylow  $p$ -subgroup of order  $p^{k-1}$ . Note that if  $\text{Aut}(\Gamma) \geq S_p \times A$ , then  $\text{Aut}(\Gamma)$  contains an element  $\beta \neq \alpha \in \text{Aut}(\Gamma) \cap \text{Aut}(G)$  as  $p \geq 3$ . Thus if  $\Gamma$  is a Cayley graph of  $G$ , then  $\Gamma \in Small(G)$  or there exists  $\beta \neq \alpha \in \text{Aut}(\Gamma) \cap \text{Aut}(G)$ .

In the latter case, by Lemma 3.1,  $\langle \alpha, \beta \rangle$  has at most  $1 + p^{k-1}/2 + p^k/4$  orbits. As  $\langle \alpha, \beta \rangle \leq \text{Aut}(G)$ ,  $\langle \alpha, \beta \rangle \leq \text{Aut}(\Gamma)$  if and only if the connection set of  $\Gamma$  is a union of orbits of  $\langle \alpha, \beta \rangle$ . We conclude that there are at most  $2^{1+p^{k-1}/2+p^k/4}$  Cayley graphs of  $G$  whose automorphism group contains  $\langle \alpha, \beta \rangle$ . By Lemma 1.2, there are at most  $|\text{Aut}(\mathbb{Z}_p^k)|$  choices for  $\alpha$ , so there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{1+p^{k-1}/2+p^k/4}$  Cayley graphs of  $G$  that are not in  $Small(G)$ . By Lemma 1.5

$$\begin{aligned} \lim_{p \rightarrow \infty} \frac{|Small(G)|}{|Cay(G)|} &\geq 1 - \lim_{p \rightarrow \infty} \frac{|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{1+p^{k-1}/2+p^k/4}}{2^{(p^k+1)/2}} \\ &\geq 1 - \lim_{p \rightarrow \infty} \frac{2^{p^k/8} \cdot 2^{1+p^{k-1}/2+p^k/4}}{2^{(p^k+1)/2}} = 1 - 0 = 1 \end{aligned}$$

$\square$

The following lemma will allow us to find a lower bound on the number of Cayley graphs of  $G$  that are not in  $Small(G)$ .



**Lemma 3.4.** *Let  $p$  be an odd prime, and  $G$  be an abelian group of prime-power order  $p^k$  such that  $G = \mathbb{Z}_{p^\ell} \times G_{p^m}$ , where  $1 \leq \ell < k$  and  $G_{p^m}$  is an abelian group of order  $p^m$ ,  $\ell + m = k$ . Define  $\iota_1, \iota_2 : G \rightarrow G$  by  $\iota_1(i, j) = (-i, j)$  and  $\iota_2(i, j) = (i, -j)$ . Then  $\langle \iota_1, \iota_2 \rangle$  has  $(2p^k + 3p^m + 3p^\ell)/8$  orbits.*

*Proof.* Clearly  $(0_{\mathbb{Z}_{p^\ell}}, 0_{G_{p^m}})$  is an orbit of  $\langle \iota_1, \iota_2 \rangle$  of length 1. Also, if  $r \neq 0$  and  $s \neq 0$ , then the orbit of  $\langle \iota_1, \iota_2 \rangle$  that contains  $(r, s)$  is  $\{(r, s), (-r, s), (r, -s), (-r, -s)\}$ . Clearly the orbit of  $\langle \iota_1, \iota_2 \rangle$  that contains  $(0, s)$ ,  $s \neq 0$ , is  $\{(0, s), (0, -s)\}$  and the orbit of  $\langle \iota_1, \iota_2 \rangle$  that contains  $(r, 0)$ ,  $r \neq 0$ , is  $\{(r, 0), (-r, 0)\}$ . As every orbit of  $\langle \iota_1, \iota_2 \rangle$  has orbits of length 1, 2, or 4, we conclude that  $\langle \iota_1, \iota_2 \rangle$  has one orbit of length 1,  $(p^\ell - 1)/2 + (p^m - 1)/2$  orbits of size 2, and  $(p^k - (p^\ell - 1)/2 - (p^m - 1)/2 - 1)/4$  orbits of length 4. Summing the number of orbits of length 1, 2, and 4, the result follows.  $\square$

**Theorem 3.5.** *Let  $G$  be an abelian group of prime-power order  $p^k$ . Then almost every Cayley graph of  $G$  whose automorphism group is not of order  $2 \cdot |G|$  is a normal Cayley graph of  $G$ . In particular,*

$$\lim_{p \rightarrow \infty} \frac{|NorCay(G) - Small(G)|}{|Cay(G) - Small(G)|} = 1.$$

*Proof.* Let  $p \geq 3$ . First suppose that  $G$  is not cyclic, with  $G = \mathbb{Z}_{p^\ell} \times G_{p^m}$ , where  $G_{p^m}$  is an abelian group of order  $p^m$  and  $\ell + m = k$ . Defining  $\iota_1$  and  $\iota_2$  as in the previous lemma, we see that  $\iota_1 \iota_2 \in \text{Aut}(\Gamma)$  for every Cayley graph of  $G$ . Applying Lemma 3.4, there are  $2^{(2p^k + 3p^m + 3p^\ell)/8}$  Cayley graphs of  $G$  whose automorphism group contains  $\langle \iota_1, \iota_2 \rangle$ , so there are at least  $2^{(2p^k + 3p^m + 3p^\ell)/8}$  Cayley graphs of  $G$  that are not in  $Small(G)$ . Clearly the number of Cayley graphs of  $G$  whose automorphism group does not contain a regular Sylow  $p$ -subgroup is at most the number of Cayley digraphs of  $G$  whose automorphism group does not contain a regular Sylow  $p$ -subgroup. By Lemma 2.7, we conclude that there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{2p^{k-1} - p^{k-2}}$  Cayley graphs of  $G$  whose automorphism group does not contain a regular Sylow  $p$ -subgroup. By Lemma 2.6, any Cayley graph of  $G$  whose automorphism group has  $G_L$  as a Sylow  $p$ -subgroup and is not a normal Cayley graph of  $G$  must have automorphism group containing a normal subgroup permutation isomorphic to  $S_p \times A$ , where  $A \leq S_{p^{k-1}}$  has an abelian Sylow  $p$ -subgroup. By Lemma 2.8, there are at most  $|\text{Aut}(\mathbb{Z}_p^k)| \cdot 2^{2p^{k-1}}$  such Cayley graphs of  $G$ . We then have that

$$\begin{aligned} \lim_{p \rightarrow \infty} \frac{|NorCay(G)|}{|Cay(G) - Small(G)|} &\geq 1 - \lim_{p \rightarrow \infty} \frac{|\text{Aut}(\mathbb{Z}_p^k)| \cdot (2^{2p^{k-1} - p^{k-2}} + 2^{2p^{k-1}})}{2^{(2p^k + 3p^m + 3p^\ell)/8}} \\ &\geq 1 - \lim_{p \rightarrow \infty} \frac{2^{p^k/8} \cdot (2^{2p^{k-1} - p^{k-2}} + 2^{2p^{k-1}})}{2^{(2p^k + 3p^m + 3p^\ell)/8}} = 1 \end{aligned}$$

by Lemma 1.5. Thus the result follows unless  $G$  is cyclic.

If  $G$  is cyclic, then first note that the result follows if  $k = 1$ , as then either  $\text{Aut}(\Gamma) < \text{AGL}(1, p)$  or  $\text{Aut}(\Gamma) = S_p$  by [1], and so there are only two non-normal Cayley graphs of the abelian group of prime order, namely  $K_p$  or its complement. For  $k \geq 2$ , observe that by Lemma 2.6, a Cayley graph  $\Gamma$  of  $G$  is either normal or has a Sylow  $p$ -subgroup that is not regular, as it is not possible for  $\text{Aut}(\Gamma)$  to contain a subgroup of the form  $S_p \times A$  as  $S_p \times A$  does not have a regular cyclic subgroup,  $A \leq S_{p^{k-1}}$  with a regular Sylow

$p$ -subgroup. If a Sylow  $p$ -subgroup of  $\text{Aut}(\Gamma)$  is not  $(\mathbb{Z}_{p^k})_L$ , then as usual there exists  $\alpha \in \text{Aut}(\mathbb{Z}_{p^k})$  such that  $\alpha$  has order  $p$  and is contained in  $\text{Aut}(\Gamma)$ . As we may assume that  $p \neq 2$ ,  $\text{Aut}(\mathbb{Z}_{p^k}) = \mathbb{Z}_{p^k}^*$  is cyclic, and so  $\text{Aut}(\mathbb{Z}_{p^k})$  contains a unique element  $\alpha$  of order  $p$ . It is straightforward to verify that  $\alpha(x) = (1 + p^{k-1})x$ , and that  $\alpha$  has  $p^{k-1}$  orbits of order 1, and  $(p^k - p^{k-1})/p$  orbits of size  $p$ . As  $\iota : \mathbb{Z}_{p^k} \rightarrow \mathbb{Z}_{p^k}$  given by  $\iota(x) = -x$  is contained in  $\text{Aut}(\mathbb{Z}_{p^k})$  and  $\text{Aut}(\Gamma)$ ,  $\iota$  has one orbit of size 1 and  $(p^k - 1)/2$  orbits of size 2, and  $\mathbb{Z}_{p^k}^*$  is cyclic, we have that  $\iota\alpha$  has one orbit of size 1,  $(p^{k-1} - 1)/2$  orbits of size 2, and  $(p^k - p^{k-1})/2p$  orbits of size  $2p$ . Then  $\iota\alpha$  has  $p^{k-1} + (1 - p^{k-2})/2$  orbits, and so there are at most  $2^{p^{k-1} + (1 - p^{k-2})/2}$  non-normal Cayley graphs of  $\mathbb{Z}_{p^k}$ ,  $p$  an odd prime and  $k \geq 2$ .

Now, let  $b \in \mathbb{Z}_{p^k}^*$  be of order  $p - 1$ , and  $\beta : \mathbb{Z}_{p^k} \rightarrow \mathbb{Z}_{p^k}$  by  $\beta(x) = bx$ . Note that  $\iota \in \langle \beta \rangle$ . If  $\beta^a(x) = x$  for  $a \geq 1$ , and  $x \neq 0$ , then  $b^a x \equiv x \pmod{p^k}$  or equivalently,  $(b^a - 1)x \equiv 0 \pmod{p^k}$ . Then  $b^a - 1 \equiv 0 \pmod{p}$  so that  $b^a = 1 + rp$  for some positive integer  $r$ . Then  $b^a$  has order a power of  $p$  and as  $|b| = p - 1$ , we must have that  $b^a = 1$  or, equivalently,  $a$  is a multiple of  $p - 1$ . We conclude that if  $x \neq 0$ , then the orbit of  $\langle \beta \rangle$  that contains  $x$  has length  $p - 1$ , and that  $\beta$  has  $1 + (p^k - 1)/(p - 1)$  orbits. Thus there are  $2^{1 + (p^k - 1)/(p - 1)}$  Cayley graphs of  $\mathbb{Z}_{p^k}$  whose automorphism group contains  $\beta$ , and so there are at least  $2^{1 + (p^k - 1)/(p - 1)}$  Cayley graphs of  $\mathbb{Z}_{p^k}$  that are not in  $\text{Small}(G)$ ,  $p \geq 3$ . Note that as  $k \geq 2$ ,  $(p^k - 1)/(p - 1) \neq 1$ . Then

$$\lim_{p \rightarrow \infty} \frac{|\text{NorCay}(G)|}{|\text{Cay}(G) - \text{Small}(G)|} \geq 1 - \lim_{p \rightarrow \infty} \frac{2^{p^{k-1} + (1 - p^{k-2})/2}}{2^{1 + (p^k - 1)/(p - 1)}} = 1.$$

□

### 4 Problems

**Conjecture 4.1.** *Almost every Cayley (di)graph whose automorphism group is not as small as possible is a normal Cayley (di)graph.*

It is difficult to determine the automorphism group of a (di)graph, so the main way to obtain examples of vertex-transitive graphs is to construct them. An obvious construction is that of a Cayley (di)graph, and the conjecture of Imrich, Lovász, Babai, and Godsil says that when performing this construction, additional automorphisms are almost never obtained. The obvious way of constructing a Cayley (di)graph of  $G$  that does not have automorphism group as small as possible is to choose an automorphism  $\alpha$  of  $G$  and make the connection set a union of orbits of  $\alpha$ . The above conjecture in some sense says that this construction almost never yields additional automorphisms other than the ones given by the construction.

There are two additional families of (di)graphs that can be considered, namely “semi-wreath products” and “deleted wreath products” - such graphs are not normal Cayley graphs provided  $p \neq 2$ . Before turning to these families, we define the wreath product of two digraphs.

**Definition 4.2.** Let  $\Gamma_1$  and  $\Gamma_2$  be digraphs. Define the *wreath product* of  $\Gamma_1$  and  $\Gamma_2$ , denoted  $\Gamma_1 \wr \Gamma_2$ , to be the graph with vertex set  $V(\Gamma_1) \times V(\Gamma_2)$  and edges set  $\{(g, h_1)(g, h_2) : h_1 h_2 \in E(\Gamma_2)\} \cup \{(g_1, h_1)(g_2, h_2) : g_1 g_2 \in E(\Gamma_1), h_1, h_2 \in V(\Gamma_2)\}$ . We say the wreath product is *trivial* if  $|V(\Gamma_1)| = 1$  or  $|V(\Gamma_2)| = 1$ .

If  $\Gamma$  is a Cayley digraph of an abelian group with connection set  $S$ , and  $\Gamma = \Gamma_1 \wr \Gamma_2$ , where  $\Gamma_1$  is a Cayley digraph of an abelian group  $G_1$  and  $\Gamma_2$  is a Cayley digraph of an abelian group  $G_2$ , then  $S - G_2$  is a union of cosets of  $G_2$ .

**Definition 4.3.** A Cayley graph  $\Gamma$  of an abelian group  $G$  is a semiwreath product if there exist subgroups  $H \leq K < G$  such that  $S - K$  is a union of cosets of  $H$ . We say that the semiwreath product is *trivial* if  $H = 1$ .

Thus if  $H = K$ , a semiwreath product is in fact a wreath product. One other comment is in order about semiwreath products. That is, it is unclear what the operands of a semiwreath product are (i.e. as defined it is not really a product). The term is used though, as many researchers refer to such graphs in this way (even if only speaking informally) as they are in some sense “almost” wreath products.

**Definition 4.4.** A Cayley graph  $\Gamma$  of an abelian group  $G$  is a deleted wreath product if  $\Gamma = (\Gamma_1 \wr \bar{K}_m) - m\Gamma_1$ , where  $\Gamma_1$  is a Cayley graph of an abelian group of order  $|G|/m$ , and  $m\Gamma_1$  is  $m$  vertex-disjoint copies of  $\Gamma_1$ .

We remark that the above definition of a semiwreath product may not be the best possible choice to capture the idea behind “semiwreath” digraphs, as the classes of semiwreath digraphs and deleted wreath products, as defined, are not disjoint. For example, the complete graph is contained in both classes, and there are other, more complicated examples that are also in both classes.

As is somewhat standard, we will refer to a Cayley (di)graph of a cyclic group of order  $n$  as a *circulant* (di)graph of order  $n$ . Baik, Feng, Song, and Xu made the following conjecture in 1998 [6]:

**Conjecture 4.5.** *All connected circulant graphs of order  $n$  are normal except for a complete graph, a wreath product of two smaller graphs, or a deleted wreath product.*

It is easy to see that this conjecture is not strictly true. Let  $C_q$  be a cycle of prime length  $q$  and  $K_p$  a complete graph of prime order  $p \neq q$ . Then  $\Gamma = C_q \wr K_p - pC_q$  is a deleted wreath product. Using [20] or the somewhat more accessible [9, Theorem 3.1], it is not difficult to see that  $\text{Aut}(\Gamma) = D_q \times S_p$ , where  $D_q$  is the dihedral group of order  $2q$ . But then  $\bar{\Gamma}$ , the complement of  $\Gamma$ , is neither a wreath product, nor a deleted wreath product, but if  $p \geq 5$  then  $\bar{\Gamma}$  is not a normal circulant graph and is certainly connected. This is not, though, a serious defect in the conjecture, as if all of the above conjectured automorphism groups were written down,  $\text{Aut}(\bar{\Gamma}) = \text{Aut}(\Gamma)$  would certainly be on the list. A more serious defect of the above conjecture is the following example.

**Example 4.6.** Let  $p$  be an odd prime and  $\Gamma$  the Cayley digraph of  $\mathbb{Z}_{p^3}$  with connection set  $S = \{\pm p, \pm 1, \pm 1 + p^2, \pm 1 + 2p^2, \dots, \pm 1 + (p - 1)p^2\}$ . Then  $\Gamma$  is a semiwreath circulant graph and is not isomorphic to a wreath product of two nontrivial graphs.

*Proof.* Clearly  $\Gamma$  is a semiwreath circulant graph with  $K$  the unique subgroup of  $\mathbb{Z}_{p^3}$  of order  $p^2$ , that is,  $K = \langle p \rangle$ , and  $H$  the unique subgroup of  $\mathbb{Z}_{p^3}$  of order  $p$ , that is  $H = \langle p^2 \rangle$ . We show that  $\Gamma$  is not isomorphic to a wreath product of two nontrivial graphs by showing that  $\text{Aut}(\Gamma) = \langle \iota, \tau, \tau^{p^2} |_{\mathcal{B}} : \mathcal{B} \in \mathcal{B} \rangle$ , where  $\iota, \tau : \mathbb{Z}_{p^3} \rightarrow \mathbb{Z}_{p^3}$  by  $\iota(i) = -i, \tau(i) = i + 1$ , and  $\mathcal{B}$  is the complete block system of  $\langle \tau \rangle$  formed by the orbits of  $\langle \tau^p \rangle$  (so the orbits of  $\langle \tau \rangle$  are just the cosets of  $K$ ). Then  $\text{Aut}(\Gamma)$  cannot be written as a nontrivial wreath product of

two groups, and so by [12, Theorem 5.7],  $\Gamma$  cannot be written as a wreath product of two nontrivial graphs.

Note that  $\text{Aut}(\Gamma)$  is clearly not a complete graph or its complement, so  $\text{Aut}(\Gamma)$  is not doubly-transitive. As  $\mathbb{Z}_{p^3}$  is a Burnside group [8, Theorem 3.5A], we must have that  $\text{Aut}(\Gamma)$  is imprimitive, admitting a nontrivial complete block system  $\mathcal{C}$ . By [26, Exercise 6.5], we have that  $\mathcal{C}$  is either formed by the orbits of  $\langle \tau^{p^2} \rangle$  or  $\langle \tau^p \rangle$ . If  $\mathcal{C}$  is formed by the orbits of  $\langle \tau^{p^2} \rangle$  (and so consists of  $p^2$  blocks of size  $p$ ), then the quotient graph  $\Gamma/\mathcal{C}$  defined by  $V(\Gamma/\mathcal{C}) = \mathcal{C}$  and  $C_1 C_2 \in E(\Gamma/\mathcal{C})$  if and only if some vertex of  $C_1$  is adjacent to some vertex of  $C_2$  is isomorphic to the circulant graph of order  $p^2$  with connection set  $T = \{\pm p, \pm 1\}$ . Using [13, Theorem 15], it is easy to verify that  $\Gamma/\mathcal{C}$  is a normal circulant graph of order  $p^2$ , and so  $\text{Aut}(\Gamma)/\mathcal{C}$  contains a normal regular cyclic subgroup. We conclude in this case that  $\text{Aut}(\Gamma)$  admits a complete block system consisting of  $p$  blocks of size  $p^2$ , necessarily formed by the orbits of  $\langle \tau^p \rangle$ . It thus suffices to only consider the case where  $\mathcal{C} = \mathcal{B}$ .

If  $\mathcal{C} = \mathcal{B}$ , then observe that  $\Gamma[B]$  is a  $p^2$ -cycle, and so has automorphism group  $D_{p^2}$ . Then  $\text{Stab}_{\text{Aut}(\Gamma)}(B)|_B \leq D_{p^2}$ , and so by [8, Exercise 1.5.10] we see that  $\text{Aut}(\Gamma)$  also admits a complete block system  $\mathcal{D}$  consisting of  $p^2$  blocks of size  $p$ , necessarily formed by the orbits of  $\langle \tau^{p^2} \rangle$ . As above,  $\Gamma/\mathcal{D}$  is the circulant digraph of order  $p^2$  with connection set  $\{\pm p, \pm 1\}$ . It follows by [13, Theorem 15] (as  $\Gamma$  cannot be written as a nontrivial wreath product as it is 4-regular and  $p > 2$ ), that  $\text{Aut}(\Gamma/\mathcal{D}) \leq \{x \rightarrow ax + b : a \in \mathbb{Z}_{p^2}^*, b \in \mathbb{Z}_{p^2}\}$ . As the only  $a \in \mathbb{Z}_{p^2}^*$  such that  $a\{\pm p, \pm 1\} = \{\pm p, \pm 1\}$  is  $a = \pm 1$  and  $x \rightarrow ax$  is an automorphism of  $\Gamma/\mathcal{D}$  if and only if  $a\{\pm p, \pm 1\} = \{\pm p, \pm 1\}$ , we see that  $\text{Aut}(\Gamma/\mathcal{D}) \cong D_{p^2}$ . Thus  $\text{Aut}(\Gamma)/\mathcal{D} = D_{p^2}$  as  $\iota \in \text{Aut}(\Gamma)$  as  $\Gamma$  is a circulant graph. As  $\text{Aut}(\Gamma)/\mathcal{D} = D_{p^2}$  and  $\text{Stab}_{\text{Aut}(\Gamma)}(B)|_B \leq D_{p^2}$ , it must be the case that  $\text{Stab}_{\text{Aut}(\Gamma)}(B)|_B = \mathbb{Z}_{p^2}$  as an involution in  $\text{Stab}_{\text{Aut}(\Gamma)}(B)|_B$  cannot be mapped to  $\iota/\mathcal{D}$  by the map  $g \rightarrow g/\mathcal{D}$  as  $\iota/B \neq 1$ . We conclude that  $\text{Aut}(\Gamma) \leq \langle \iota, \tau, \tau^{p^2} \rangle|_B : B \in \mathcal{B}$ . It is not difficult to see that  $\langle \tau, \tau^{p^2} \rangle|_B : B \in \mathcal{B} \leq \text{Aut}(\Gamma)$ , and then the result follows.  $\square$

We believe that the two types of counterexamples to the Conjecture 4.5 are the only possible counterexamples for Cayley (di)graphs of abelian groups. We make the following conjecture, which would be quite useful in verifying Conjecture 4.1.

**Conjecture 4.7.** *Let  $\Gamma$  be a Cayley (di)graph of an abelian group  $G$ . Then one of the following is true:*

- $\Gamma$  is a normal Cayley (di)graph of  $G$ ,
- $\Gamma$  is a semiwreath product, or
- the automorphism group of  $\Gamma$  is same as the automorphism group of a deleted wreath product.

It is not overly difficult to show using [23, Theorem 2.3] (this result is basically a translation of work done on Schur rings [14, 21, 22] into the language of group theory, and this result was independently obtained in [11] for the special case of circulants of square-free order) that the preceding conjecture is true provided that  $G$  is cyclic, and so the two types of counterexamples to Conjecture 4.5 presented above are indeed the only possible types of counterexamples provided that  $G$  is cyclic. We remark that the preceding conjecture is known to be false for some nonabelian groups, as for some such groups it is possible for

a Cayley (di)graph to have an almost simple simply primitive automorphism group (see [24]).

Finally, we would like to finish with an additional problem.

**Problem 4.8.** For an abelian group  $G$ , does there exist a natural collection  $\mathcal{F}$  of families of Cayley (di)graphs of  $G$  and a partial order  $\preceq$  on  $\mathcal{F}$  such that every Cayley (di)graph of  $G$  is contained in some element of  $\mathcal{F}$  and if  $F_1 \preceq F_2$  and there is no  $F_3$  such that  $F_1 \preceq F_3 \preceq F_2$ , then almost every Cayley (di)graph of  $G$  that is not in  $F_1$  is in  $F_2$ ?

## 5 Acknowledgement

The author is indebted, as usual, to the anonymous referees for their careful reading of this manuscript, and their thoughtful suggestions for improvement. The manuscript is much improved thanks to their efforts.

## References

- [1] B. Alspach, Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, *J. Combinatorial Theory Ser. B* **15** (1973), 12–17.
- [2] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.
- [3] L. Babai, Infinite digraphs with given regular automorphism groups, *J. Combin. Theory Ser. B* **25** (1978), 26–46.
- [4] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* **11** (1980), 257–270.
- [5] L. Babai and C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15.
- [6] Y.-G. Baik, Y. Feng, H.-S. Sim and M. Xu, On the normality of Cayley graphs of abelian groups, *Algebra Colloq.* **5** (1998), 297–304.
- [7] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič and L. A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc.* **66** (2002), 325–333.
- [8] J. D. Dixon and B. Mortimer, *Permutation groups*, Vol. 163 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.
- [9] E. Dobson, On the proof of a theorem of Pálffy, *Electron. J. Combin.* **13** (2006), #16.
- [10] E. Dobson, On overgroups of regular abelian  $p$ -groups, *Ars Math. Contemp.* **2** (2009), 59–76.
- [11] E. Dobson and J. Morris, On automorphism groups of circulant digraphs of square-free order, *Discrete Math.* **299** (2005), 79–98.
- [12] E. Dobson and J. Morris, Automorphism groups of wreath product digraphs, *Electron. J. Combin.* **16** (2009), #17.
- [13] E. Dobson and D. Witte, Transitive permutation groups of prime-squared degree, *J. Algebraic Combin.* **16** (2002), 43–69.
- [14] S. A. Evdokimov and I. N. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, *Algebra i Analiz* **14** (2002), 11–55.
- [15] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256.

- [16] C. D. Godsil, GRRs for nonsolvable groups, in: *Algebraic methods in graph theory*, Vol. I, II (Szeged, 1978), Vol. 25 of Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam, 1981, 221–239.
- [17] D. Gorenstein, *Finite groups*, Harper & Row Publishers, New York, 1968.
- [18] B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.
- [19] L. A. Kalužnin and M. H. Klin, Some numerical invariants of permutation groups, *Latvišsk. Mat. Ežegodnik (Vyp. 18)* (1976), 81–99.
- [20] M. H. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings, in: *Algebraic methods in graph theory*, Vol. I, II (Szeged, 1978), Vol. 25 of Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam, 1981, 405–434.
- [21] K. H. Leung, S. H. Man, On Schur rings over cyclic groups. II, *J. Algebra* **183** (1996), 273–285.
- [22] K. H. Leung and S. H. Man, On Schur rings over cyclic groups, *Israel J. Math.* **106** (1998), 251–267.
- [23] C. H. Li, Permutation groups with a cyclic regular subgroup and arc transitive circulants, *J. Algebraic Combin.* **21** (2005), 131–136.
- [24] D. Marušič, R. Scapellato, Classifying vertex-transitive graphs whose order is a product of two primes, *Combinatorica* **14** (1994), 187–201.
- [25] G. Sabidussi, Vertex-transitive graphs, *Monatsh. Math.* **68** (1964), 426–438.
- [26] H. Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964.
- [27] M.-Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319.